REMARKS

Claims 11, 13, 14, 16-19, and 22-28 are pending. The Examiner's reconsideration of the rejection in view of the remarks is respectfully requested.

Claims 11, 13, 14, 16, 18 and 22-26 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. (USPAN 2001/0050990) in view of Abbondanzio (US 2003/0188176).

As an initial matter, Claim 13 is addressed by the Examiner under the rejection but is not specifically listed among in the heading of the rejection. Applicants believe that the Examiner intended to include Claim 13 in the rejection and consider Claim 13 below in view of Sudia and Abbondanzio.

Claims 11, 22 and 23 are the independent claims.

Claims 11 and 22 claim, *inter alia*, executing "said signed authorized boot code having a verified digital signature by branching to a copy of said signed authorized boot code in said protected memory, said signed authorized boot code including instructions for performing a boot process for a computer device comprising the processor." Claim 23 claims, *inter alia*, "a processor comprising includes inline cryptography and integrity hardware for executing boot code in signal communication with said protected memory executing said signed authorized code from the protected memory for booting the computing device after verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory." Claims 11, 22 and 23 have been clarified to specify that the signed authorized code is executed by the processor and that the code embodies a boot process (see for example, paragraphs [0022-0024] of the published application).

Referring to Claims 11, 22 23, the combination of Sudia and Abbondanzio is believed to be improper. Respectfully, the proposed combination requires that the processor of a server to be booted executes boot code. The proposed combination is counter to the express teachings of Abbondanzio, wherein the boot code is executed on a network, e.g., deployment server or customer boot server, different than a server blade to be booted (see FIG. 2). That is, it is the express intended purpose of Abbondanzio to perform the execution of boot code off of the system to be booted. Consider paragraph [0058], which teaches:

> In step 606, the one or more server blades 110 determined to **boot from either deployment server 130 or customer boot server 206** may boot from the appropriate device, e.g., deployment server 130, customer boot server 206. In one embodiment, the one or more server blades 110 determined to boot from either deployment server 130 or customer boot server 206 may boot from the appropriate device over a public network, e.g., campus LAN 205 (FIG. 2).

In view of the foregoing, the proposed combination of references renders the Abbondanzio reference unsatisfactory for an intended purpose.

Even assuming, arguendo, that one could combine the references, the combination fails to teach or suggest all of the claimed limitations.

Referring to Claims 11 and 22, Sudia teaches a cryptographic system with a key escrow feature (see Abstract). Sudia teaches how to perform a desired upgrade instruction in a tamper-resistance trusted device (see paragraph [0250]). The upgrade process presumes that the trusted device is booted. Sudia does not consider how to perform the upgrade process, much less execute the upgrade firmware, at boot time. For example, Sudia fails to teach that a processor includes inline cryptography and integrity hardware for executing boot code, essentially as claimed in

Claim 23. Consider that Sudia teaches that the "basic cryptographic library routines" are stored in firmware (see paragraphs [0097-0099]). Sudia makes use of cryptography software or code without the ability to perform such operations prior to booting the trusted device.

Abbondanzio teaches methods for remotely booting devices by remotely configuring authentication parameters instead of manually installing them on the devices to be booted (see Abstract).

The proposes combination of Sudia and Abbondanzio is characterized by the Examiner as enabling the use of "Sudia system of installing new or additional firmware code with Abbondanzio method of transmitting a sign boot code as a more secure way to transmit boot code" (see page 4, Office Action).

Respsectfully, the combination of Sudia and Abbondanzio fails to teach or suggest how to execute signed authorized code that embodies a boot process. Note that Claims 11 and 22 recited "executing further comprises performing inline decryption of the copy of said signed authorized boot code in said protected memory**.**" That is, the combination of Sudia and Abbondanzio fails to teach or suggest methods for performing a cryptographic process prior to booting a device, by the device. That is, according to the claimed limitations of Claims 11 and 22, "said signed authorized boot code including instructions for performing a boot process for a **computer device comprising the processor**."

More particularly, Abbondanzio teaches a method for booting to a network, which is different than the server to be booted. The process of executing boot code is not performed by the server to be booted. Therefore, the combination of Sudia and Abbondanzio fails to teach or suggest all of the limitations of Claims 11 and 22.

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 17, 19, 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Sudia and Morgan teach or suggest all of the limitations of Claims 17, 19, 27 and 28.

Claims 17 and 19 depend from Claim 11. Claims 27 and 28 depend from Claim 23. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Reconsideration of the rejection is respectfully requested.

For the forgoing reasons, the application, including Claims 11, 13, 14, 16-19, and 22-28, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: June 17, 2011

By: /Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889